ANTI-MONEY LAUNDERING/ COMBATING TERRORIST FINANCING GUIDELINE

For

Financial Institutions Licensed

Under

The Financial Institutions Act

And

The International Financial Services Act

Central Bank of Barbados
October 2006
Amended September 2007

Table Of Contents

ANTI-MONEY LAUNDERING/COMBATING TERRORIST FINANCING

1.0 INTRODUCTION

The global threats of money laundering and the financing of terrorism have led financial sector regulators and financial institutions to strengthen their vigilance in support of the efforts of governments to more easily detect attempts to launder money and finance terrorism and to minimise the possibility that their jurisdictions or institutions become involved. Effective enforcement of policies to deter money laundering and the financing of terrorism should, inter alia, enhance the integrity of the financial system and reduce incentives for the commission of crime within the jurisdiction.

The Central Bank of Barbados (Bank), in furtherance of its responsibility for the regulation and supervision of licensees under the Financial Institutions Act 1996-16 (FIA) and the International Financial Services Act 2002-5 (IFSA), has revised its Know Your Customer (KYC) guideline to provide guidance to licensees on how they can fulfil their obligations in relation to the Money Laundering and Financing of Terrorism (Prevention and Control) Act 2002-6 (MLFTA).

The guideline, which is being issued in conjunction with the Anti-Money Laundering Authority (Authority) pursuant to its powers under Section 22(F) of MLFTA, replaces the 2001 KYC guideline and is designed to reflect the changes in international standards pertaining to money laundering, the development of standards related to the financing of terrorism following the events of September 11, 2001 and changes in the domestic legislative environment.

The development and implementation of effective customer due diligence systems and monitoring mechanisms are essential to help combat money laundering and the financing of terrorism. This guideline sets out the expectations of the Bank and the Authority in relation to the minimum standards for anti-money laundering and the combating of the financing of terrorism (AML/CFT) practices by all licensees and, together with the MLFTA, it will form an integral part of the framework used by the Bank in assessing how licensees implement their AML/CFT policies.

Section 8(1)(f) of the MLFTA obligates all licensees to comply with this guideline. The guideline contains both advisory and obligatory requirements. Advisory matters are expressed by way of the term ”may” and financial institutions are permitted to implement alternative but effective measures in these circumstances. Mandatory requirements are expressed using the term “should”.

2.0 APPLICATION

This guideline[1] applies to all entities that are incorporated in Barbados and that are licensed under the FIA and IFSA. These institutions should ensure that, at a minimum, this guideline is also implemented in their branches and subsidiaries abroad. Licensees should inform the Bank and the Authority if the local applicable laws and regulations prohibit the implementation of this Guideline.

While other financial sector regulators have issued their own guidance notes to their sectors, the Bank recognises that other persons and entities, whose business involves money transmission services, investment services or any other service of a financial nature, are also vulnerable to the threat of money laundering and terrorist financing. **See Appendix 1**. These persons and entities interface directly with licensees. It is recommended that they consider the issues embodied in this guideline and, to this end, they may also avail themselves of the relevant portions of this guideline.

3.0 MONEY LAUNDERING AND FINANCING OF TERRORISM

3.1 Money Laundering

Money laundering has been defined as the act or attempted act to disguise the source of money or assets derived from criminal activity. It is the effort to transform “dirty” money, into “clean” money. The money laundering process often involves:

i. The **placement** of the proceeds of crime into the financial system, sometimes by techniques such as structuring currency deposits in amounts to evade reporting requirements or co-mingling currency deposits of legal and illegal enterprises;
ii. The **layering** of these proceeds by moving them around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail; and
iii. **Integrating** the funds into the financial and business system so that they appear as legitimate funds or assets.

3.2 Financing of Terrorism

Terrorism is the act of seeking for political, religious or ideological reasons to intimidate or compel others to act in a specified manner. A successful terrorist group, much like a criminal organization, is generally able to obtain sources of funding and develop means of obscuring the links between those sources and the uses of the funds. While the sums needed are not always large and the associated transactions are not necessarily complex, terrorists need to ensure that funds are available to purchase the goods or services needed to commit terrorist acts. In some cases, persons accused of terrorism may commit crimes to finance their activities and hence

[1] For the purposes of this guideline, general references to money laundering should be interpreted as references to money laundering and/or the financing of terrorism.

transactions related to terrorist financing may resemble money laundering.

4.0 INTERNATIONAL INITIATIVES

The Basel Committee (Basel) and the Financial Action Task Force (FATF) have issued international standards on measures which should form part of a licensee's AML/CFT programme. In October 2001, the Committee issued a paper entitled ***Customer Due Diligence for Banks***, which was subsequently reinforced by a ***General Guide to Account Opening and Customer Identification*** in February 2003. In addition, Basel recognized the global challenge for financial institutions to implement sound KYC policies and procedures using a group wide approach. It issued ***Consolidated KYC Risk Management*** in October 2004, requiring each group to develop a global risk management programme supported by policies that embrace group wide KYC standards.

The **FATF Forty Recommendations** were revised in June 2003 and, with the ***Nine Special Recommendations on Terrorist Financing, which were*** issued in October 2004, apply to both money laundering and to terrorist financing. Further guidance was issued on ***Special Recommendations on Terrorist Financing and the Self Assessment Exercise*** (March 2002), ***Guidance for Financial Institutions in Detecting Terrorist Financing*** (April 2002) and Interpretative Notes II (***Criminalizing the Financing of Terrorism and the Associated Money Laundering***, III (***Freezing and Confiscating Terrorist Assets***), VI (***Alternative Remittance***), VII (***Wire Transfers***), VIII (***Non-Profit Organisations***) and IX (***Cash Couriers***).

Together, these standards provide the international framework of measures for combating money laundering and terrorist financing. Other useful references are provided in **Appendix 2**.

5.0 LEGISLATIVE AND REGULATORY FRAMEWORK

The Government of Barbados has enacted several pieces of legislation aimed at preventing and detecting drug trafficking, money laundering, terrorist financing and other serious crimes. These comprise**:**

- Drug Abuse (Prevention and Control) Act, 1990-14, CAP131;
- Proceeds of Crime Act, 1990-13, CAP143;
- Mutual Assistance in Criminal Matters Act, 1992, CAP140A;
- Anti-Terrorism Act, 2002-6; and
- Money Laundering and Financing of Terrorism (Prevention and Control) Act, 2002-6, CAP129.

The MLFTA indicates that a financial institution engages in money laundering if it fails to take reasonable steps to implement or apply procedures to control or combat money laundering and it confers responsibility for the supervision of financial institutions[2] to the Authority, which was established in August 2000. A Financial Intelligence Unit has been established to carry out the Authority's supervisory function over financial institutions. As the operational arm of the Authority, its responsibilities, inter alia, include:

i. Receiving suspicious or unusual transactions reports from financial institutions;
ii. Investigating suspicious or unusual transactions reports;
iii. Instructing financial institutions to take steps that would facilitate an investigation; and
iv. Providing training to financial institutions in respect of record keeping obligations and reporting obligations under the MLFTA.

Where a licensee is uncertain about how to treat an unusual or suspicious transaction, it should speak directly to the FIU for preliminary guidance and then make a report as appropriate. Where the FIU believes on reasonable grounds that a transaction involves the proceeds of crime, the FIU will send a report for further investigation to the Commissioner of Police.

The Bank, the supervisory and regulatory agency for institutions licensed under the FIA and IFSA, assesses these licensees' AML/CFT framework and compliance with the MLFTA through periodic onsite inspections. Where deficiencies are identified in policy framework or operations of the control framework for managing the licensee's AML/CFT programme, the Bank will agree with the licensee on a time period to address the shortcomings. However, if the Bank is concerned by the seriousness of non-compliance and/or the lack of responsiveness to previous findings, the Bank may enforce its powers under Section 11(1)(d) of the FIA or Section 15(1)(c) of the IFSA.

In addition, the Bank is required by law to provide any information that it has in its possession, which the FIU deems useful for an investigation that is being conducted for the purposes of the MLFTA.

From time to time, the Bank, in conjunction with the AMLA, will amend this Guideline but licensees should, as part of their risk management practices, stay current with emerging developments as they relate to AML/CFT and upgrade their AML/CFT programme where necessary.

6.0 THE ROLE OF THE BOARD AND SENIOR MANAGEMENT

Licensees must see AML/CFT as part of their overall risk management strategy. Money laundering and terrorist financing expose a licensee to transaction, compliance and reputation risk. For financial institutions convicted of money laundering or terrorist financing, there are considerable costs. Licensees therefore should establish an effective AML/CFT programme that

[2] Offences and penalties under the MLFTA are set out in Appendix 3.

minimises these risks and potential costs.

The Board of Directors has ultimate responsibility for the effectiveness of the licensee's AML/CFT framework. The Board has an oversight role designed to ensure inter alia that there is compliance with all the relevant laws and regulations and international standards. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

Directors and senior management should be aware that:

i. The use of a group wide policy does not absolve directors of their responsibility to ensure that the policy is appropriate for the licensee and compliant with Barbadian law, regulations and guidelines. Failure to ensure compliance by the licensee with the requirements of the MLFTA may result in significant penalties for directors and the licensee (**See Appendix 3**);
ii. Subsidiaries and branches of licensees including those domiciled outside of Barbados are expected to, at a minimum, comply with the requirements of Barbados MLFTA and this guideline; and
iii. Where some of licensee's operational functions are outsourced, the licensee retains full responsibility for compliance with local laws, regulations and guidelines.

Directors should therefore demonstrate their commitment to an effective AML/CFT programme by:

i. Understanding the statutory duties placed upon them, their staff and the entity itself;
ii. Approving AML/CFT policies and procedures that are appropriate for the risks faced by the licensee. Evidence of consideration and approval of these policies should be reflected in the board minutes;
iii. Appointing an individual within the organisation for ensuring that the licensee's AML/CFT procedures are being managed effectively; and
iv. Seeking assurance that the licensee is in compliance with its statutory responsibilities as it relates to AML/CFT. This includes reviewing the reports from Compliance on the operations and effectiveness of compliance systems. See Section 9.0.

Senior management is responsible for the development of sound risk management programmes and for keeping directors adequately informed about these programmes and their effectiveness. These programmes, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, should be formally documented and, at a minimum, irrespective of whether the licensee receives funds from third parties or not, should provide for:

i. The development of internal policies, procedures and controls for inter alia:

    a. The opening of customer accounts and verification of customer identity;

b. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);
c. Determining business relationships that the licensee will not accept;
d. The timely detection of unusual and suspicious transactions, and reporting to the Authority;
e. Internal reporting; and
f. Record retention.

ii. The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, and research of unusual transactions and reporting of suspicious activities;
iii. An ongoing training programme designed to ensure adherence by employees to the legal and internal procedures, and familiarity with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;
iv. Designation of a compliance officer at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program, receive internal reports and issue suspicious transaction reports to the Authority; See Section 8.0.
v. Establishment of management information/reporting systems to facilitate aggregate and group wide monitoring;
vi. An effective independent risk-based oversight function to test and evaluate the compliance program; and
vii. Screening procedures for hiring, and ongoing systems to promote high ethical and professional standards to prevent the licensee from being used for criminal activity.

Policies should be periodically reviewed for consistency with the business model, and product and service offering. Special attention should be paid to new and developing technologies.

6.1 Risk-Based Approach

The Bank recognises the diversity of the institutions it regulates and it will seek to establish that, overall, processes appropriate to institutions are in place and operating effectively. All licensees should therefore design an AML/CFT framework that satisfies the needs of their institution, taking into account:

i. The nature and scale of the business;
ii. The complexity, volume and size of transactions;
iii. The degree of risk associated with each area of operation;
iv. Type of customer (e.g. whether ownership is highly complex, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group);
v. Type of product/service (e.g. whether private banking, one-off transaction, mortgage);
vi. Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);

vii. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking or corruption, whether the customer is subject to regulatory or public disclosure requirements); and
viii. Value of account and frequency of transactions.

Financial institutions may apply customer due diligence standards on a risk sensitive basis depending on the type of customer, business relationship or transaction. Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems. Alternatively, licensees should apply enhanced due diligence to customers (Section 7.4) where the risk of being used for money laundering or terrorist financing is high.

Financial institutions should document a risk-based approach in their AML/CFT programmes. This approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This should be evidenced by categorisation of the customer base, products and services by risk rating (e.g. low, medium, high) and identification of assigned actions by risk types.

While each licensee will determine the number and name of risk categories, the fundamental issue is for the adoption of reasonable criteria for assessing risks. In addition to "Red Flags" appended to this guideline, typologies of money laundering and terrorist financing schemes are available[3] to assist in risk categorisation.

Licensees should ensure that systems are in place to periodically test the accuracy of the assignment of the customer base to risk categories and that the requisite due diligence is being followed. In addition, licensees should periodically review their risk categories as typologies evolve on practices by money launderers and terrorists.

7.0 CUSTOMER DUE DILIGENCE

Customer due diligence is an essential element of the effort to prevent the financial system from being used to perpetrate money laundering and terrorist financing. Licensees are ultimately responsible for verifying the identity of their customers. In this regard, licensees must avoid the acceptance of anonymous accounts or accounts in fictitious names. If licensees maintain numbered accounts, they must ensure compliance with this guideline.

As part of their due diligence process, licensees should:

i. Establish procedures for obtaining identification information on new customers so as to be satisfied that a prospective customer is who he claims to be;

[3] For example, www.fatf-gafi.org.

ii. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset[4] of a business relationship. This process should include, where appropriate:

    a. Taking reasonable measures to understand the ownership and control structure of the customer;
    b. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and
    c. Discontinuing the transaction, if customer documentation information is not forthcoming at the outset of the relationship.

iii. Employ enhanced due diligence procedures for high risk customers or transactions (Section 7.4);
iv. Update identification records, on a risk-focussed basis, to ensure that all existing customer records are current and valid and conform to any new requirements (Section 7.6);
v. Monitor account activity throughout the life of the business relationship; and
vi. Review the existing records if there is a material change in how the account is operated or if there are doubts about previously obtained customer identification data.

For the purposes of this guideline, the licensee should seek to identify the customer and all those who exercise control over the account/transaction. A customer includes:

i) A person or entity that maintains an account with the licensee;
ii) A person or entity on whose behalf an account is maintained i.e. beneficial owner;
iii) The beneficiaries of transactions conducted by professional intermediaries such as lawyers, accountants, notaries, business introducers or any other professional service providers; or
iv) Any person or entity connected with a financial transaction that can pose a significant risk to the licensee, including persons establishing business relations, purporting to act on behalf of a customer or conducting transactions such as:

- Opening of deposit accounts;
- Entering into fiduciary transactions;
- Renting safe-deposit boxes;
- Requesting safe custody facilities; and
- Occasional transactions exceeding thresholds as discussed below or linked transactions under this benchmark, and all occasional wire transfers.

For the purpose of this guideline, an occasional transaction is one that is conducted by a person without an account or facility at the licensee. Occasional transactions include:

a. Encashment of cheques drawn on the licensee;

[4] For the purpose of this guideline, the outset of the relationship is the earlier of acceptance of the signed application / proposal, or the first receipt of funds from the customer.

b. Exchange of coins for cash;
c. Purchase of foreign currency for holiday travel; and
d. Currency exchanges e.g. bureau de change and cambios.

Due diligence should be undertaken on, inter alia:

- Occasional transactions over BDS$10,000 or its equivalent in foreign currency, whether conducted in a single or multiple operations that appear to be linked;
- Occasional wire transfers over BDS$2,000 or its equivalent in foreign currency; and
- All currency exchange transactions over BDS$2000 or its equivalent in foreign currency.

The extent of identity information and verification of occasional transactions below these thresholds[5] is dependent on the materiality of the transaction and the degree of suspicion.

At a minimum, a licensee should:

a. Identify and verify[6] the persons conducting occasional transactions below the above thresholds. (See Section 7.4.9 on wire/funds transfers);
b. Maintain an effective system to monitor for abuse of occasional transactions; and
c. Establish clear instructions for the timely reporting of unusual and suspicious occasional transactions.

In effecting the due diligence process, licensees should:

i) Whenever possible, require prospective customers to be interviewed in person. Exceptions to this are outlined in Sections 7.4.3 and 7.4.4;
ii) In verifying customer identity, use official or other reliable source documents, data or information to verify the identity of the beneficial owner prior to opening the account or establishing the business relationship. Identification documents which do not bear a photograph or signature and which are easily obtainable (e.g. birth certificate and driver's licence) are not acceptable as the sole means of identification. Customer identity can be verified using a combination of methods such as those listed at **Appendix 4.** Verification may involve the use of external electronic databases.
iii) In instances where original documents are not available, only accept copies that are certified by an approved person. See **Appendix 5**. Approved persons should print their name clearly, indicate their position or capacity together with a contact address and phone number;
iv) If the documents are unfamiliar, take additional measures to verify that they are genuine e.g. contacting the relevant authorities; and
v) Determine through a risk analysis of the type of applicant and the expected size and activity

[5] See Section 8.0 for discussion on profiling and transaction limits.
[6] At a minimum, identification information may consist of the customer's name and address, which is verified by valid photo-bearing ID with a unique identifier.

of the account, the extent and nature of the information required to open an account. Examples of documentation for different types of customers are set out in Sections 7.1 to 7.5.

Generally, licensees should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, where it would be essential not to interrupt the normal conduct of business (e.g. non face-to-face business and securities transactions), verification may be completed after establishment of the business relationship. Should licensees determine this to be an acceptable risk, they should retain control of any funds received until verification requirements have been met. If the requirements are not met, and the licensee determines that the circumstances give rise to suspicion, it should make a report to the Authority (See Section 8).

Where there is a suspicion that a transaction relates to money laundering or the financing of terrorism, licensees should be cognizant of tipping off a customer when conducting due diligence. The licensee should make a business decision whether to open the account or execute the transaction as the case may be, but a suspicious report should be submitted to the Authority.

7.1 Personal Customer

A licensee should obtain relevant information on the identity of its customer and seek to verify some of the information on a risk basis, through the use of reliable, independent source documents, data or information to prove to its satisfaction that the individual is who that individual claims to be. The basic information should include:

a. True name and permanent residential address;
b. Valid photo-bearing identification, with unique identifier, (e.g. passport, national identification card, driver's licence);
c. Date and place of birth and nationality (if dual, should be indicated);
d. Occupation;
e. Contact details e.g. telephone number, fax number and e-mail address;
f. Purpose of the account; and
g. Signature.

In addition, the licensee may obtain any other information deemed appropriate and relevant e.g. source of funds and estimated account turnover.

The licensee should determine the degree of verification to be undertaken on a risk basis. In some instances, verification may be satisfied by maintaining current photo-bearing identification with a unique identifier (e.g. passport, national identification card).

Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted if certified by persons listed in **Appendix 5.**

7.1.1 Unavailability of Identity Documents

There may be circumstances where some types of customers are unable to supply the identity documents at Section 7.1. Such customers include the elderly, the disabled, students, minors and individuals dependent on the care of others. Licensees should determine what alternate identity documentation to accept and verification to employ. Where applicable, the following should be among documentation obtained:

a) A letter or statement from a person listed at **Appendix 5** that the person is who he/she states;
b) Confirmation of identity from another regulated institution in a jurisdiction with equivalent standards;
c) Confirmation(s) from the student's workplace, school, college or university; and
d) Identity information on the adult opening the account, and a birth certificate, or national registration card for the account holder.

7.2 Corporate Customer

To satisfy itself as to the identity of the customer, the licensee should obtain:

a. Name of corporate entity;
b. Principal place of business and registered office;
c. Mailing address;
d. Contact telephone and fax numbers;
e. Identity information (See Section 7.1) on the beneficial owners of the entity. This information should extend, as far as practicable, to identifying those who ultimately own and control the company and should include anyone who is giving instructions to the licensee to act on behalf of the company. However,
    i. If the company is publicly listed on a recognised stock exchange and not subject to effective control by a small group of individuals, identification on shareholders is not required;
    ii. If the company is a private, identity should be sought on persons with a minimum of 10% shareholding.
f. Identity information (See Section 7.1) on directors and officers who exercise effective control over the business and are in a position to override internal procedures / control mechanisms and, in the case of bank accounts, the signatories to the account;
g. Description and nature of business;
h. Purpose of the account, source of funds and the estimated account activity;
i. Certified copy of the Certificate of Incorporation, authenticated where the body is incorporated outside of Barbados, or Certificate of Continuance pursuant to Section 352 or 356.2 of the Companies Act or Certificate of Registration where the body was incorporated abroad but registered under the Companies Act;
j. Certified Copy of the Memorandum and Articles of Association of the entity;

k. By-laws and any other relevant corporate documents filed with the Registrar of Corporate Affairs and Intellectual Property;
l. Board resolution authorising the opening of the account and conferring authority on signatories to the account; and
m. Recent financial information or audited statements.

In addition, the licensee may obtain any other information deemed appropriate. For example, where it is deemed necessary, a licensee may also request the financial statements of parent or affiliate companies, or seek evidence that the entity is not in the process of being dissolved or wound-up. It should request this information, particularly for non-resident companies, where the corporate customer has no known track record or it relies on established affiliates for funding.

7.3 Partnership/Unincorporated Business

Partnerships and unincorporated businesses should meet the relevant requirements set out in Section 7.1. Each partner should be identified as well as immediate family members with ownership control. In addition to providing the identification documentation for partners/controllers and authorised signatories, where a formal partnership arrangement exists, there should be a mandate from the partnership authorising the opening of an account.

7.4 Enhanced Due Diligence

A licensee may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A licensee may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.

The licensee's policy framework should therefore include a description of the types of customers that are likely to pose a higher than average risk and procedures for dealing with such applications. High-risk customers should be approved by senior management and stringent documentation, verification and transaction monitoring procedures should be established. Applying a risk-based approach, enhanced due diligence for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:

a) An evaluation of the principals;
b) A review of current financial statements;
c) Verification of the source of funds;
d) Verification of source of wealth;
e) The conduct of reference checks;
f) Checks of electronic databases; and
g) Periodic reporting to the Board about high risk accounts.

Types of situations requiring enhanced due diligence include the below:

7.4.1 Trust Clients

Licensees should take reasonable measures to obtain information about the true identity of the persons on whose behalf an account is opened or a transaction is conducted. This applies especially if there are any doubts as to whether or not these clients or customers are acting on their own behalf.

At a minimum, the licensee should obtain the following[7]: -

a. Name of trust;
b. Nature / type of trust;
c. Country of establishment;
d. Identity of the trustee(s), settlor(s), protector(s)/controller(s) or similar person holding power to appoint or remove the trustee and where possible the names or classes of beneficiaries;
e. Identity of person(s) with powers to add beneficiaries, where applicable; and
f. Identity of the person providing the funds, if not the ultimate settlor.

Depending on the type or nature of the trust, it may be impractical to obtain all of the above at the onset of the relationship e.g. unborn beneficiaries. In such cases, discretion should be exercised and documented in a manner consistent with the requirements in this guideline. In all circumstances, there should be verification of beneficiaries before the first distribution of assets. Further, verification of protectors/controllers should be undertaken the earlier of the first instance of exercise of power conferred by the trust instrument or the issue of instruction to an advisor to provide advice.

Ongoing due diligence should be applied in the context of changes in any of the parties to the trust, revision of the trust, addition of funds, investment of trust funds or distribution of trust assets/provision of benefits out of trust assets.

Verification of the identity of the trust is satisfied by obtaining a copy of the creating instrument and other amending or supplementing instruments.

Licensees are required to inform the Bank and the FIU when applicable laws and regulations in the domicile where trusts are established, prohibit the implementation of this guideline.

[7] These minimum requirements apply whether the licensee is a named trustee or is providing services to a trust.

7.4.2 Non-Profit Organisations (NPOs)

NPOs differ in size, income, structure, legal status, membership and scope. They engage in raising or disbursing funds for charitable, religious, cultural, educational, social or fraternal purposes or for carrying out other types of "good works". NPOs can range from large regional, national or international charities to community-based self-help groups. They also include research institutes, churches, clubs, and professional associations. They typically depend in whole or in part on charitable donations and voluntary service for support. While terrorist financing may occur through small, non-complex transactions, enhanced due diligence may not be necessary for all clients that are small organisations, dealing with insignificant donations for redistribution among members. Licensees should therefore, determine the risk level of activities in which the NPO is engaged.

To assess the risk, a licensee should focus inter alia on:

a. Purpose, ideology or philosophy;
b. Geographic areas served (including headquarters and operational areas);
c. Organisational structure;
d. Donor and volunteer base;
e. Funding and disbursement criteria (including basic beneficiary information);
f. Record keeping requirements; and
g. Its affiliation with other NPOs, Governments or groups.

The licensee should also include the following in the identity records:

a) Evidence of registration of the home and local operation, where applicable;
b) Identity of all signatories to the account; and
c) Identity of board members and trustees, where applicable.

As part of the verification process, licensees should confirm that the organisation is registered under the appropriate laws and with the tax authorities and should carry out due diligence against publicly available terrorist lists. As part of ongoing monitoring activity, licensees should examine whether funds are being sent to high-risk countries.

7.4.3 Non Face-to-Face Customers

The rapid growth of financial business by electronic means increases the scope for non-face -to-face business and increases the risk of criminal access to the financial system. Customers may use the internet, the mail service or alternative means because of their convenience or because they wish to avoid face-to-face contact, Consequently, special attention should be paid to risks associated with new and developing technologies. Customers may complete applications but licensees should satisfy the requirements in this section before establishing a business relationship.

When accepting business from non-face-to-face customers, in order to prove to its satisfaction that the individual is who that individual claims to be, licensees should:

a. Obtain documents certified by approved persons listed at **Appendix 5**;
b. Ensure that all company documents are signed by the Company Secretary;
c. Request additional documents to complement those which are required for face-to-face customers, including more than one photo bearing ID;
d. Make independent contact with the customer, for example by telephone on a listed business or other number; and
e. Request third party introduction e.g. by an introducer as noted in Section 7.4.4.

In addition, the licensee may:

a) Carry out employment checks (where applicable) with the customer's consent through a job letter or verbal confirmation on a listed business or other number;
b) Require the first payment to be carried out through an account in the customer's name with another bank subject to equivalent customer due diligence standards; and
c) Obtain any other information deemed appropriate.

Where initial checks fail to identify the customer, additional checks should be independently confirmed and recorded. If the prospective customer is required to attend a branch to conduct the first transaction, or to collect account documentation or credit/debit cards, then valid photo bearing identification should be obtained at that time.

Where a licensee or its subsidiary initiates transactions in its role as a securities broker or in the sale of mutual funds without establishing face-to-face contact and obtaining all of the relevant documentation, it should make all efforts to obtain such information as soon as possible. In accepting such transactions, licensees should:

i. Set limits on the number and aggregate value of transactions that can be carried out;
ii. Indicate to customers that failure to provide the information within a set timeframe, may trigger the termination of the transaction; and
iii. Consider submitting a suspicious report.

7.4.4 Introduced Business

A licensee may rely on other regulated third parties to introduce new business in whole or in part but the ultimate responsibility remains with the licensee for customer identification and verification. Licensees should:

a. Document in a written agreement the respective responsibilities of the two parties;
b. Satisfy itself that the regulated entity or introducer has in place KYC practices at least equivalent to those required by Barbados law and the licensee itself;

c. Obtain copies of the due diligence documentation provided to the introducer prior to the commencement of the business relationship;
d. Satisfy itself that an introducer continues to conform to the criteria set out above (e.g. conduct periodic reviews);
e. Consider terminating the relationship where an introducer fails to provide the requisite customer identification and verification documents; and

f. Consider terminating the relationship with an introducer who is not within the licensee's group, where there are persistent deviations from the written agreement.

When a prospective customer is introduced from within a licensee's group, provided the identity of the customer has been verified by the introducing regulated parent company, branch, subsidiary or associate in line with the standards set out in the guideline, it is not necessary to re-verify the identification documents unless doubts subsequently arise about the veracity of the information. The licensee should however, retain copies of the identification records in accordance with the requirements in the MLFTA. Licensees should obtain written confirmation from a group member confirming completion of verification. **See Appendix 6**.

7.4.5 Professional Service Providers

Professional service providers act as intermediaries between clients and the licensee and they include lawyers, accountants and other third parties that act as financial liaisons for their clients. When establishing and maintaining relationships with professional service providers, a licensee should:

a. Adequately assess account risk and monitor the relationship for suspicious or unusual activity;
b. Understand the intended use of the account, including the anticipated transaction volume, products and services used, and geographic locations involved in the relationship; and
c. Obtain the identity of the beneficial owners of the client funds where it is not satisfied that the intermediary has in place due diligence procedures equivalent to the standard of this guideline.

Where pooled accounts are managed by:

a. Providers on behalf of entities such as mutual funds and pension funds; or
b. Lawyers or stockbrokers representing funds held on deposit or in escrow for several individuals, and funds being held are not co-mingled (i.e. there are sub-accounts), the licensee should identify each beneficial owner. Where funds are co-mingled, the licensee should take reasonable measures to identity the beneficial owners. Subject to the Bank's approval, the latter is not required where the provider employs at a minimum, equivalent due diligence standards as set out in this guideline and has systems and controls to allocate the assets to the relevant beneficiaries. Licensees should apply the criteria at Section 7.4.4 in conducting due diligence on providers.

Financial institutions should observe guidance from the FIU regarding attorney-client accounts.

7.4.6 Politically Exposed Persons (PEPs)

Concerns about the abuse of power by public officials for their own enrichment and the associated reputation and legal risks which licensees may face have led to calls for enhanced due diligence on such persons. The FATF defines a PEP as a foreign senior political figure[8], their immediate family[9] and close associates. However, identifying PEPs can be problematic.

A licensee should:

i. Develop policies, procedures and processes such as the use of electronic databases to assess whether a customer is or has become a PEP;
ii. Take reasonable measures to establish the source of wealth and the source of funds of PEPs;
iii. Exercise greater scrutiny and monitoring of all PEP accounts; and
iv. Require senior management to determine whether to continue the relationship where an existing customer subsequently becomes or is found to be a PEP.

In addition to the identity information normally requested for personal customers, the following information on a PEP should be gathered:

a. Estimated net worth, including financial statements;
b. Information on immediate family members or close associates having transaction authority over the account; and
c. References or other information to confirm the reputation of the client.

7.4.7. Corporate Vehicles

Barbados law prohibits companies from issuing shares in bearer form. Where a licensee decides that companies with nominee shareholders represent an acceptable business risk, they should exercise care in conducting transactions. Licensees should ensure they can identify the beneficial owners of such companies and should immobilise bearer shares as a means of monitoring the identity of such companies by, for example, requiring custody by:

a. The licensee, or its subsidiary, regulated affiliate, parent or holding company;
b. A recognized regulated financial institution in a jurisdiction with equivalent AML/CFT standards; and

[8] **Senior political figure** is a senior figure in the executive, legislative, administrative, military or judicial branches of a government, a senior figure of a political party, or a senior executive of a government-owned corporation. It includes any corporate entity, partnership or trust relationship that has been established by, or for the benefit of a senior political figure.
[9] **Immediate family** typically includes the person's parents, siblings, spouse, children and in-laws.

c. Requiring the prior approval before shares can be exchanged.

7.4.8 Correspondent Banking

Correspondent banking relates to the provision of banking services by one bank (correspondent) to another bank, usually domiciled overseas (respondent). A correspondent bank faces enhanced risks, as it may have no relationship with the customers of the respondent bank. Examples of correspondent banking include wire/fund transfers, trade related and treasury/money market activities.

The decision to approve a respondent relationship should depend inter alia on the licensee's assessment of the counterpart's money laundering and terrorist financing prevention and detection systems and controls, and the quality of bank supervision and regulation in the counterpart's country. Licensees offering cross-border wire or fund transfers should avoid correspondent and respondent banking relations with shell banks[10].

Licensees that offer correspondent banking services should conduct due diligence on their respondent banks on a risk basis.

A licensee should obtain the following on the respondent bank:

a. Information on the ownership, and board and senior management;
b. Assessment of the risk profile (consider the location and nature of major business activities);
c. Satisfy itself that there is an equivalent AML/CFT programme in place;
d. Confirmation that the respondent does not maintain business relations with shell banks;
e. Assessment of the quality of bank supervision and regulation in the respondent's country; and
f. Evidence of senior management's approval before establishing the relationship.

7.4.9 Wire/Funds Transfer

For the purposes of this guideline, wire transfer and funds transfer refer to any transaction carried out on behalf of an originator[11] person through a licensee by electronic means for availability to a beneficiary person at another financial institution. The originator and beneficiary may be the same person.

[10] A **shell bank** is a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.
[11] The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

The degree of enhanced due diligence depends on the licensee's role in the wire transfer and the size and origin or destination of the funds. These circumstances are set out below:

i) Where it acts as the ordering financial institution, the licensee should obtain, retain and verify the full originator information, i.e. the originator's name, account number (or unique identifier where the originator is not an account holder), and address[12] for wire transfers in any amount. Verification of existing customers should be refreshed where there are doubts about previously obtained information.

ii) As ordering financial institution, the licensee should include in cross-border wire transfers above the BDS$2,000 threshold[13], full originator information. Batch transfers[14] that include cross-border wire transfers sent by a money/value transfer service provider should be treated as cross-border transfers.

iii) As the ordering financial institution conducting a domestic transfers above the BDS$2000 threshold, the licensee should include full originator information. However, the licensee may send only the originator's account number (or unique identifier) where full originator information can be made available to:
   a. The receiving financial institution and the Bank within three (3) business days of receipt of a request; and
   b. Domestic law enforcement authorities upon request.

iv) As ordering financial institution, batch transfers that include cross-border transfers may be treated as domestic wire transfers, provided that the requirements applicable to domestic transfers are met.

v) Where it acts as an intermediary financial institution, the licensee should ensure that all originator information from cross-border transfers of any amount, remain with the related domestic transfers. Where difficulties arise in maintaining the information, then all information received from the ordering financial institution should be retained for five years. (See Footnote 13).

vi) Where it acts as the beneficiary financial institution, the licensee should apply a risk-based system to the review transfers for complete originator information and the reporting of unusual or suspicious activity.

The requirements are not applicable to the following types of payments:

i) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, the necessary information should be included in the message; and

ii) Financial institution-to-financial institution transfers where both the originator and the

[12] It is permissible to substitute national identity number/customer identity number/date and place of birth.
[13] The FATF requires financial institutions to have appropriate systems in place to facilitate the capture and transfer of all required information by no later than **31/12/2006**.
[14] In general, only routine transactions should be batched.

beneficiary are financial institutions acting on their own behalf.

Where a relationship is deemed high risk e.g. located in a high-risk jurisdiction, further to standard due diligence, a licensee should undertake a more detailed understanding of the:

i) AML/CFT programme of the respondent bank and its effectiveness;
ii) Review effectiveness of the respondent's group programme;
iii) Respondent's owners, director and senior managers; and
iv) Ownership structure.

7.5 Reduced Customer Due Diligence

As discussed in Section 6.1, the licensee's policy document should clearly define the risk categories/approach adopted and associated due diligence, monitoring and other requirements. A licensee may apply reduced due diligence to a customer provided it satisfies itself that the customer is of such a risk level that qualifies for this treatment. Such circumstances are set out below:

i) Where an application to conduct business is made by:

   a. An entity regulated by the Bank under IFSA or FIA;
   b. An entity regulated by the Securities Commission of Barbados;
   c. An entity regulated by the Supervisor of Insurance in Barbados;
   d. An entity regulated by the Registrar of Co-operatives in Barbados;
   e. The Government of Barbados; or
   f. A statutory body.

ii) Where there is a transaction or series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.

iii) Where an existing customer opens a new account unless the condition described at Section 7.6, sub-item (ii) holds. However, if the source of funds/wealth originates from an external source, or from a country where, for example, it is believed that there is a high level of drug trafficking or corruption, reduced due diligence should not apply.

iv) Where a licensee acquires the business of another regulated entity, whether in Barbados or elsewhere, and it is satisfied that the due diligence standards of the acquired institution are at least equivalent to that set in this guideline, it need not re-verify the customers.

If the licensee is not satisfied that equivalent standards have been followed or the customer records are not consistent with the requirements of this guideline, the licensee should seek to identify and verify the identity of customers who do not have existing relationships with the licensee

along the lines set out in Section 7.6.

7.6 Retrospective Due Diligence

Where the identity information held on existing customers does not comply with the requirements of this guideline, licensees are required to develop a risk-based programme for ensuring compliance. Licensees should:

i. Record their non-compliant business relationships, noting what information or documentation is missing;
ii. Establish a framework for effecting retrospective due diligence, including the setting of deadlines for the completion of each risk category. The timing of retrofitting can be linked to the occurrence of a significant transaction, a material change in the way that an account is operating, or doubts about previously obtained customer due diligence data; and
iii. Establish policies for coping with an inability to obtain information and documentation, including terminating the relationship and making a suspicious report.

Where a licensee deems on the basis of risk and materiality, that it is not practical to retrofit a customer (e.g. the settlor has died; the account is inactive or dormant), exemption of such accounts should be approved by the compliance officer and senior management, ratified by the board and documented on the individual's file.

8.0 UNUSUAL & SUSPICIOUS TRANSACTIONS

Suspicious transactions are financial transactions that give rise to reasonable grounds to suspect that they are related to the commission of a money laundering or terrorism offence. These transactions may be complex, unusual or large or may represent an unusual pattern. This includes significant transactions relative to the relationship, transactions that exceed prescribed limits or a very high account turnover that is inconsistent with the expected pattern of transactions. In some instances, the origin of the transaction may give rise to suspicion. For examples of "Red Flags" see **Appendix 7**.

A pre-requisite to identifying unusual and suspicious activity is the profiling of customers and determination of consistent transaction limits. Unusual transactions are not necessarily suspicious, but they should give rise to further enquiry and analysis. In this regard, licensees should examine, to the extent possible, the background and purpose of transactions that appear to have no apparent economic or visible lawful purpose, irrespective of where they originate.

Licensees should develop procedures to assist in the identification of unusual or suspicious activity in all types of business transactions, products and services offered (for example wire transfers, credit/debit cards and ATM transactions, lending, trust services and private banking).

A licensee should:

i. Develop effective manual &/or automated systems to enable staff to monitor, on a solo, consolidated and group-wide basis, transactions undertaken throughout the course of the business relationship and identify activity that is inconsistent with the licensee's knowledge of the customer, their business and risk profile; and
ii. Determine customer specific limits based on an analysis of the risk profile of customers, the volume of transactions and the account turnover. This may give rise to multiple limits and/or aggregate limits on a consolidated basis.

Licensees should not grant blanket exemptions and should:

i. Clearly document their policy for the granting of such exemptions including the qualifying criteria for exemption, officers responsible for preparing and authorizing exemptions, the basis for establishing threshold limits, review of exempt customers and procedures for processing transactions.
ii. Maintain authorised exempt lists showing threshold limits established for each qualifying customer; and
iii. Monitor currency exchanges and international wire transfers.

For the purposes of this guideline, a transaction includes an attempted or aborted transaction.

8.1 Internal Reporting Procedures

To facilitate the detection of suspicious transactions, a licensee should:

i. Require customers to declare the source and/or purpose of funds for business transactions in excess of threshold limits, or such lower amount (i.e. wire transfers) as the licensee determines, to ascertain the legitimacy of the funds. **Appendix 8** indicates a specimen of a Declaration Source of Funds (DSOF) form. Where electronic reports are employed instead of the form, they should capture the information included on the Appendix and should be signed by the customer;
ii. Develop written policies, procedures and processes to provide guidance on the reporting chain and the procedures to follow when identifying and researching unusual transactions and reporting suspicious activities;
iii. Identify a suitably qualified and experienced person to whom unusual and suspicious reports are channelled. The person should have direct access to the appropriate records to determine the basis for reporting the matter to the Authority (See Section 8.2);
iv. Require its staff to document in writing their suspicion about a transaction; and
v. Require documentation of internal enquiries.

8.2 External Reporting

Licensees are required by law to report forthwith to the Authority where the identity of the person involved, the transaction or any other circumstance concerning that transaction lead the licensee to have reasonable grounds to suspect that a transaction:

i) Involves proceeds of crime to which the MLFTA applies;
ii) Involves the financing of terrorism; or
iii) Is of a suspicious or an unusual nature.

In addition, pursuant to the United Nations Resolutions on terrorist financing, licensees should freeze any funds or other assets held for individuals or organisations listed on the UN list of persons connected to terrorism, and submit a report to the Authority. This list may be accessed at **www.un.org**[15].

Where a suspicious report has been filed with the Authority, and further unusual or suspicious activity pertaining to the same customer or account arises, licensees should file additional reports with the Authority.

Licensed financial institutions, their directors, officers, employees and agents are protected under the MLFTA from any action, suit or proceedings for breach of any restriction on disclosure of information, if they report suspicious activity in good faith to the Authority, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred. It is against the law for employees, directors, officers or agents of a licensee to disclose that a suspicious transaction report or related information on a specific transaction has been reported to the Authority.

Reports should be in the format determined by the FIU (**See Appendix 9**). However, where a matter is considered urgent, an initial report may be made by contacting the FIU by telephone or e-mail.

Where a person is a client of both the licensee and another group member, and a suspicious report is prepared by the latter, the Barbados FIU should be notified.

9.0 COMPLIANCE AND AUDIT

All licensees should designate a suitably qualified person with the appropriate level of authority, seniority and independence as Compliance Officer. The Compliance Officer should be independent of the receipt, transfer or payment of funds, or management of customer assets and should have timely and uninhibited access to customer identification, transaction records and other relevant information. The powers and reporting structure of the officer should be conducive to the

[15] http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm

effective and independent exercise of duties.

The Compliance Officer should:

i. Undertake responsibility for developing compliance policies;
ii. Develop a programme to communicate policies and procedures within the entity;
iii. Monitor compliance with the licensee's internal AML programme;
iv. Receive internal reports and consider all such reports;
v. Issue, in his/her own discretion, external reports to the Authority as soon as practicable after determining that a transaction warrants reporting;
vi. Monitor the accounts of persons for whom a suspicious report has been made;
vii. Establish and maintain on-going awareness and training programmes for staff at all levels;
viii. Establish standards for the frequency and means of training;
ix. Report at least annually to the board of directors (or relevant oversight body in the case of branch operations) on the operations and effectiveness of the systems and controls to combat money laundering and the financing of terrorism;
x. Review compliance policies and procedures to reflect changes in legislation or international developments;
xi. Participate in the approval process for high-risk business lines and new products, including those involving new technologies; and
xii. Be available to discuss with the Bank or the FIU matters pertaining to the AML/CFT function.

The internal audit department should carry out reviews to evaluate how effectively compliance policies are being implemented. Such reviews should be carried out on a frequency consistent with the licensee's size and risk profile. The review process should identify and note weaknesses in policies and procedures, corrective measures and ensure timely follow-up of actions.

The Bank recognises, however, that the designation of a Compliance Officer or the creation of an internal audit department may create difficulties for some small licensees. Where the licensee is part of a larger regulated financial or mixed conglomerate, the Group Compliance Officer or Group Internal Audit may perform the compliance and/or internal audit services. Where this is not possible, a licensee may, subject to the Bank's agreement, outsource the operational aspects of the compliance or internal audit function to a person or firm that is not involved in the auditing or accounting functions of the licensee. Notwithstanding, the responsibility for compliance with the MLFTA and the guideline remains that of the licensee and the requirements of this section will extend to the agent. A licensee should have a local control function and be in a position to readily respond to the Bank and FIU on AML/CFT issues.

10.0 RECORD-KEEPING

To demonstrate compliance with the MLFTA and to facilitate investigations undertaken by the FIU, licensees should establish a document retention policy that provides for the maintenance of a broad spectrum of records, including those related to customer identification, business transactions, internal and external reporting and training.

Licensees should retain all records of business transactions exceeding BDS$10,000 or the equivalent in foreign currency and should ensure that linked transactions, which are individually below this limit, but with an aggregate value exceeding this amount, are monitored and appropriately recorded. Records obtained on occasional transactions should also be retained.

Licensees should maintain these records for a minimum of **five years** after the termination of the business transaction, or the business relationship, whichever is applicable.

However, it may be necessary for licensees to retain records, until such time as advised by the FIU or High Court, for a period exceeding the date of termination of the last business transaction where:

i. There has been a report of a suspicious activity; or
ii. There is an on-going investigation relating to a transaction or client.

Licensees should ensure that records held by an affiliate outside Barbados at a minimum, comply with the requirements of Barbados law and this guideline.

Records should be retained in a format, including electronic, scanned or microfilm, that would facilitate reconstruction of individual transactions (including the amounts and types of currency involved) so as to provide, if necessary, evidence for prosecution of criminal activity and to enable licensees to comply swiftly with information requests from the FIU. This applies whether or not records are stored off the premises of the licensee.

When a licensee merges with or takes over another entity, it should ensure that the records described above can be readily retrieved. Where the records are kept in a contractual relationship by an entity other than a licensee, the licensee is responsible for retrieving those records before the end of the contractual arrangement.
The nature of records that should be retained is set out below:

10.1 Customer Records

In order to comply with Section 8 (1) (a) of the MLFTA, licensees should retain:

i. Copies or records of customer identification, including those obtained through the conduct of enhanced due diligence;

ii. Account files, account statements and business correspondence; and
iii. All business transaction records, domestic and international, of all transactions exceeding BDS$10,000 or its equivalent in foreign currency, and of all occasional transactions over the thresholds stated in Section 7.0.

In relation to business transactions, the requirements on the type of records to be retained are set out in Section 8(3) of the MLFTA.

10.2 Internal and External Records

Licensees should maintain records related to unusual and suspicious transaction reports. These should include:

i. All reports made by staff to the Compliance Officer;
ii. The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;
iii. Consideration of those reports and of any action taken; and
iv. Reports by the Compliance officer to senior management and board of directors.

10.3 Training Records

In order to provide evidence of compliance with Sections 8(1) and 10 of the MLFTA, at a minimum, a licensee should maintain the following information:

- Details and contents of the training programme provided to staff members;
- Names of staff receiving the training;
- Dates that training sessions were held;
- Test results carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

11.0 TRAINING AND AWARENESS

An integral element of the fight against money laundering and the financing of terrorism is the awareness of those charged with the responsibility of identifying and analysing potential illicit transactions. Licensees should, therefore, establish ongoing employee training programmes. Training should be targeted at all employees but added emphasis should be placed on the training of the Compliance Officer and the compliance and audit staff because of their critical role in sensitising the broader staff complement to AML/CFT issues and ensuring compliance with policy and procedures.

Licensees, therefore, should:

i. Develop an appropriately tailored training and awareness programme consistent with their size, resources and type of operation to enable their employees to be aware of the risks associated with money laundering and terrorist financing, to understand how the institution might be used for such activities, to recognise and handle potential money laundering or terrorist financing transactions and to be aware of new techniques and trends in money laundering and terrorist financing;
ii. Clearly explain to staff the laws, the penalties for non-compliance, their obligations and the requirements concerning customer due diligence and suspicious transaction reporting;
iii. Formally document, as part of their anti-money laundering policy document, their approach to training, including the frequency, delivery channels and content;
iv. Ensure that all staff members are aware of the identity and responsibilities of the Compliance Officer and/or the Reporting Officer to whom they should report unusual or suspicious transactions;
v. Establish and maintain a regular schedule of new and refresher programmes, appropriate to their risk profile**,** for the different types of training required for:

    a. New hire orientation;
    b. Operations staff;
    c. Supervisors;
    d. Board and senior management; and
    e. Audit and compliance staff.

vi. Obtain an acknowledgement from each staff member on the training received;
vii. Assess the effectiveness of training[16]; and
viii. Provide all staff with reference manuals/materials that outline their responsibilities and the institution's policies. These should complement rather than replace formal training programmes.

11.1 Content and Scope of the Training Programme

A licensee's overall training programmes should cover topics pertinent to its operations. Training should be general as well as specific to the area in which the trainees operate. As staff members move between jobs, their training needs for AML/CFT may change. Training programmes should, inter alia, incorporate references to:

i. Relevant money laundering and terrorism financing laws and regulations;
ii. Definitions and examples of laundering and terrorist financing schemes;
iii. How the institution can be used by launderers or terrorists;

[16] Assessment methods include written or automated testing of staff on training received, use of evaluation forms by recipients of training, confirmation of delivery of training according to plan, and review of the contents of training.

iv. The importance of adhering to customer due diligence policies, the processes for verifying customer identification and the circumstances for implementing enhanced due diligence procedures;
v. The procedures to follow for detection of unusual or suspicious activity across lines of business and across the financial group;
vi. The completion of unusual and suspicious transaction reports;
vii. Treatment of incomplete or declined transactions; and
viii. The procedures to follow when working with law enforcement or the FIU on an investigation.

12.0 PRE-EMPLOYMENT BACKGROUND SCREENING

The ability to implement an effective AML/CFT programme depends in part on the quality and integrity of staff. Licensees should, therefore, undertake due diligence on prospective staff members. The senior management of a licensee should:

i. Verify the applicant's identity;
ii. Develop a risk-focussed approach to determining when pre-employment background screening is considered appropriate or when the level of screening should be increased, based upon the position and responsibilities associated with a particular position. The sensitivity of the position or the access level of an individual staff member may warrant additional background screening, which should include verification of references, experience, education and professional qualifications.
iii. Maintain an ongoing approach to screening for specific positions, as circumstances change, or for a comprehensive review of departmental staff over a period of time. Internal policies and procedures should be in place (e.g. codes for conduct, ethics, conflicts of interest) for assessing staff; and
iv. Have a policy that addresses appropriate actions when pre-employment or subsequent due diligence detects information contrary to what the applicant or employee provided.

APPENDICES

Appendix 1

Coverage of Entities

Although MLFTA applies to all persons and businesses, additional administrative requirements are placed on financial institutions. According to Section 2 (1) of MLFTA, a *financial institution* means:

- Any person who carries on business under FIA; and Includes:
- A deposit taking institution;
- Any person whose business involves money transmission services, investment services or any other services of a financial nature;
- A credit union within the meaning of the *Co-operatives Societies Act*;
- A building society within the *Building Societies Act*;
- A friendly society within the meaning of the *Friendly Societies Act*;
- An insurance business within the meaning of the *Insurance Act*;
- An offshore bank within the meaning of the *Offshore Banking Act* (repealed to form IFSA);
- An exempt insurance company within the meaning of the *Exempt Insurance Act*;
- An international business company within the meaning of the *International Business Companies Act*;
- A society with restricted liability within the meaning of the *Societies with Restricted Liability Act*;
- A foreign sales corporation within the meaning of the *Barbados Foreign Sales Corporation Act*;
- A mutual fund, mutual funds administrator and a mutual fund manager; and
- International trusts within the meaning of the *International Trusts Act*.

Appendix 2

Additional References

Name of Organisation	Website Address / Link
Basel Committee on Banking Supervision • Core Principles for Effective Banking Supervision • Core Principles Methodology • Customer Due Diligence for Banks • Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering – December 1998	http://www.bis.org/bcbs/ http://www.bis.org/publ/bcbs30.pdf http://www.bis.org/publ/bcbs61.pdf http://www.bis.org/publ/bcbs85.htm#pgtop http://www.bis.org/publ/bcbsc137.pdf
Caribbean Financial Action Task Force (CFATF)	www.cfatf.org
Commonwealth Secretariat	http://www.thecommonwealth.org
Egmont Group for Financial Intelligence Units	http://www.egmontgroup.org
Financial Action Task Force (FATF)	http://www.fatf-gafi.org
Financial Stability Forum	http://www.fsforum.org
International Association of Insurance Supervisors	http://www.iaisweb.org
International Monetary Fund	www.imf.org
International Organisation of Securities Commission	http://www.iosco.org
Interpol (Interpol's involvement in the fight against international terrorism)	http://www.interpol.com/public/terrorism/default.asp
Organisation of American States – CICAD	http://www.cicad.oas.org
The Financial Crime Enforcement Network (FINCEN)	http://www.fincen.gov/af_main.html
The World Bank	http://www.worldbank.org
United Nations	http://www.un.org
United Nations – International Money Laundering Information Network	http://www.imolin.org
United Nations – Security Council Resolutions	http://www.un.org/documents/scres.htm
US Department of the Treasury, Comptroller of the Currency Administrator of National Banks (Money Laundering: A Banker's Guide to Avoiding Problems)	http://www.occ.treas.gov/launder/origc.htm
Wolfsberg Group	http://www.wolfsberg-principles.com/index.html

Appendix 3

Summary of Money Laundering and Terrorism Offences

Area	Description of Offence	Description of Fine	Section of Legislation
Reporting Obligations	Failure of licensee to make a report on a suspicious transaction to the Authority.	$100,000 on directors jointly and severally	Section 8 (4) MLFTA
	Failure of a licensee to maintain business transactions records.	$100,000 on directors jointly and severally	Section 8(5) MLFTA
	Failure of a person to report transfers out of Barbados or transfers Barbadian currency or foreign currency into Barbados, of more than BDS$10,000 without Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 8A(6) MLFTA
	Failure by a person to report receiving more than BDS$10,000 in Barbadian currency (or foreign equivalent) without the Exchange Control permission.	Summary conviction - $10,000 or 2 years imprisonment Conviction on indictment - $200,000 or 5 years imprisonment	Section 8A(6) MLFTA
Interference in the Line of Duty	The obstruction, hindrance, molestation or assault to any member of the Authority, constable or other person in performing duties under the Act.	$50,000 or imprisonment of 2 years or both	Section 16 MLFTA
Money Laundering Offences	Engagement of money laundering.	Summary conviction - $200,000 or 5 years imprisonment or both. Conviction on indictment - $2,000,000 or 25 years imprisonment or both. Forfeiture of licence for financial institution	Section 20 (1) MLFTA Section 12

Area	Description of Offence	Description of Fine	Section of Legislation
	Providing assistance to engage in money laundering.	Summary conviction - $150,000 or 3 years imprisonment or both. Conviction on indictment - $1,500,000 or 15 years imprisonment or both	Section 20(2) MLFTA
	A body of persons (corporate or unincorporated) whether as a director, manager, secretary or other similar officer engaging in a money laundering offence.	Subject to trial and punishment accordingly.	Section 21 MLFTA
Disclosure of Information	Disclosure of information on a pending money laundering investigation. Falsifying, concealing, destruction or disposal of information material to investigation or order.	$50,000 or 2 years imprisonment or both	Section 22(4) MLFTA
	Disclosure or publication of the contents of any document, communication or information in the course of duties under this Act.	$50,000 or 5 years imprisonment or both.	Section 22A (2) MLFTA.
Terrorism Offences	Provision or collection funds or financial services to persons to be used to carry out an offence as defined in the listed treaties[17] or any other act.	Conviction on indictment to 25 years imprisonment.	Section 4(1) Anti-Terrorism Act

[17] Treaties respecting Terrorism: Convention for the Suppression of Unlawful Seizure of Aircraft, Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons including Diplomatic Agents, International Convention against the taking of Hostages, Convention on the Physical Protection of Nuclear Material, Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, Convention for the suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf and the International Convention for the Suppression of Terrorists Bombings.

Area	Description of Offence	Description of Fine	Section of Legislation
	Provision of assistance or involve in the conspiracy to commit a terrorist offence.	Conviction on indictment and principal offender punished accordingly.	Section 3 of ATA
	A terrorist offence committed by a person responsible for the management or control of an entity located or registered in Barbados, or otherwise organised under the laws of Barbados.	$2,000,000 notwithstanding that any criminal liability has been incurred by an individual directly involved in the commission of the offence or any civil or administrative sanction as imposed by law.	Section 5 of ATA

Appendix 4

Verification Examples

A. Personal Clients

- Confirm the date of birth from an official document (e.g. birth certificate).
- Confirm the permanent address (e.g. utility bill, tax assessment, bank statement, letter from a public notary).
- Contact the customer e.g. by telephone, letter, email to confirm information supplied
- Confirming the validity of the official documents provided through certification by an authorised person.
- Confirm the permanent and/ business residence through credit agencies, home visits
- Obtain personal references from third parties and existing customers in writing.
- Contact issuers of references.
- Confirmation of employment.

B. Corporate Customers & Partnerships

- Review of current audited information (preferably audited).
- Obtain statements of affairs, bank statements, confirmation of net worth from reputable financial advisers.
- Seek confirmation from a reputable service provider(s).
- Confirm that the company is in good standing.
- Undertake enquiries using public and private databases.
- Obtain prior banking and commercial references, in writing.
- Contact issuers of references.
- Onsite visitations.
- Contact the customer e.g. by telephone, letter, email to confirm information supplied.

C. Trusts and Fiduciary Clients

- Seek confirmation from a reputable service provider(s).
- Obtain prior bank references.
- Access public or private databases.

Appendix 5
Amended September 2007

Approved Persons For Certification of Customer Information

In keeping with Section 7.4.3 on non face-to-face customers, licensees should only accept customer information that has been certified by:

Any of the below persons in Barbados, or their counterparts in jurisdictions with at least equivalent AML/CFT standards:

- Notary Public
- *Senior Public Servant
- Member of the Judiciary
- Magistrate
- Attorney-At-Law with a valid practising certificate
- Accountant who is a member of a national professional association
- Senior banking officer (at least management level)
- Senior Officer of a Consulate/Embassy/High Commission of the country issuing the passport

*In Barbados, this refers to the:

- Registrar/Deputy Registrar of Corporate Affairs and Intellectual Property
- Registrar/Deputy Registrar, Supreme Court
- Registrar/Deputy Registrar, Land Registry
- Chief Personnel Officer, Personnel Administration Division
- Permanent Secretary, Ministry of Home Affairs
- Permanent Secretary, Chief of Protocol, Ministry of Foreign Affairs
- Chief/Deputy Chief Immigration Officer
- Private Secretary to the Governor General
- Commissioner/Deputy Commissioner/Assistant Commissioner/Senior Superintendent of Police
- Superintendent/Assistant Superintendent of Prisons

Appendix 6

Confirmation of Customer Verification of Identity

Part A - Personal Customers

Full Name of Customer: (Mr/Mrs/Ms)
……..

Known Aliases:……

Identification:……...

Current Permanent Address:……

Date of Birth:……. Nationality:……...

Country of Residence:……

Specimen Customer Signature Attached: Yes No

Part B - Corporate & Other Customers

Full Name of Customer**:**……..

Type of Entity: ……..

Location & domicile of Business: ……

Country of Incorporation: ……

Regulator / Registrar: ……

Names of Directors: ……

……

Names of majority beneficial owners:……..

……

Appendix 6 (cont'd)

Confirmation of Customer Verification of Identity

Part C

We confirm that the customer is known to us.	Yes	No	
We confirm that the identity information is held by us.	Yes	No	
We confirm that the verification of the information meets			
- the requirements of Barbados law and AML/CFT Guideline.	Yes		No
We confirm that the applicant is acting on his own behalf and - not as a nominee, trustee or in a fiduciary capacity for any - other person.	Yes	No	N/A

Part D

Customer Group Name:……..

Relation with Customer:……

Part E

Name & Position of Preparing Officer:……
(Block Letters)

Signature & Date:……..

Name & Position of Authorising Officer:……
(Block Letters)

Signature & Date:……..

Appendix 7

Red Flags

There are a myriad of ways in which money laundering or terrorism financing may occur. Below is a non–exhaustive list of "Red Flags" that may warrant closer attention. Financial institutions are encouraged to refer to the FATF and Egmont Group for typology reports and sanitised cases on money laundering and terrorist financing schemes, respectively.

General

If the Client:

- Does not want correspondence sent to home address.
- Shows uncommon curiosity about internal systems, controls and policies.
- Over justifies or explains the transaction.
- Is involved in activity out-of-keeping for that individual or business.

If the client:

- Produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Provides insufficient, false, or suspicious information, or information that is difficult or expensive to verify.

Economic Purpose

- Transaction is unnecessarily complex for its stated purpose.
- Activity is inconsistent with what would be expected from declared business.
- Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer's business.

Cash Transactions

If the Client:

- Starts conducting frequent cash transactions in large amounts when this has not been a normal activity in the past.
- Frequently exchanges small bills for large ones.
- Deposits small amounts of cash on different successive occasions, in such a way that on each occasion the amount is not significant, but combine to total a very large amount. (i.e. “smurfing”).
- Consistently makes cash transactions that are just under the reporting threshold amount in a apparent attempt to avoid the reporting threshold.
- Stated occupation is not in keeping with the level or type of activity (e.g. a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).
- Unusually large deposits or withdrawals of cash by an individual or a legal entity whose apparent business activities are normally carried out using cheques and other monetary instruments.

Deposit Activity

- Account with a large number of small cash deposits and a small number of large cash withdrawals.
- Funds are being deposited into several accounts, consolidated into one and transferred outside the country.
- Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.
- Establishment of multiple accounts, some of which appear to remain dormant for extended periods.
- Account that was reactivated from inactive or dormant status suddenly exhibits significant activity.

- Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.
- Multiple deposits are made to a client's account by third parties.
- Deposits or withdrawals of multiple monetary instruments, particularly if the instruments are sequentially numbered.

Cross-border Transactions

- Deposits followed within a short time by wire transfers to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.
- Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money laundering system.
- Immediate conversions of funds transfers into monetary instruments in the name of third parties.
- Frequent sending and receiving of wire transfers, especially to or from countries considered high risk for money laundering or terrorist financing, or with strict secrecy laws. Added attention should be paid if such operations occur through small or family-run banks, shell banks or unknown banks.
- Large incoming or outgoing transfers, with instructions for payment in cash.
- Client makes frequent or large electronic funds transfers for persons who have no account relationship with the institution.
- Client instructs you to transfer funds abroad and to expect an equal incoming transfer.
- Client sends frequent wire transfers to foreign countries, but business does not seem to have connection to destination country.
- Wire transfers are received from entities having no apparent business connection with client.

Personal Transactions

- Client has no employment history but makes frequent large transactions or maintains a large account balance.
- Client has numerous accounts and deposits cash into each of them with the total credits being a large amount.
- Client frequently makes automatic banking machine deposits just below the reporting threshold.
- Increased use of safety deposit boxes. Increased activity by the person holding the boxes. The depositing and withdrawal of sealed packages.
- Third parties make cash payments or deposit cheques to a client's credit card.
- Client has frequent deposits identified as proceeds of asset sales but assets cannot be substantiated.

Corporate and Business Transactions

- Accounts have a large volume of deposits in bank drafts, cashier's cheques, money orders or electronic funds transfers, which is inconsistent with the client's business.
- Accounts have deposits in combinations of cash and monetary instruments not normally associated with business activity.
- Unexplained transactions are repeated between personal and business accounts.
- A large number of incoming and outgoing wire transfers take place for which there appears to be no logical business or other economic purpose, particularly when this is through or from locations of concern, such as countries known or suspected to facilitate money laundering activities.

Lending

- Customer suddenly repays a problem loan unexpectedly, without indication of the origin of the funds.
- Loans guaranteed by third parties with no apparent relation to the customer.
- Loans backed by assets, for which the source is unknown or the value has no

relation to the situation of the customer.

- Default on credit used for legal trading activities, or transfer of such credits to another company, entity or person, without any apparent justification, leaving the bank to enforce the guarantee backing the credit.
- Use of standby letters of credit to guarantee loans granted by foreign financial institutions, without any apparent economic justification.

Securities Dealers

- Client frequently makes large investments in stocks, bonds, investments trusts or the like in cash or by cheque within a short time period, which is inconsistent with the normal practice of the client.
- Client makes large or unusual settlements of securities in cash.
- Client is willing to deposit or invest at rates that are not advantageous or competitive.

Accounts Under investigation

- Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in a court or other competent national or foreign authority in connection with fraud, terrorist financing or money laundering.
- Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority with fraud, terrorist financing or money laundering.

Appendix 8

Declaration Source Of Funds/Wealth

Customer Name Or Business:……..

Current Address:……..

Account Number:……

Identification:……..

Amount Of Transaction & Currency:

Description/Nature Of Business Transaction:

Deposit Monetary Instrument Currency Exchange Wire Transfer Credit/Debit Card
ATM Loan Investment Trust Settlement / Distribution Other (Specify)

Source of Funds / Wealth:

……
……
……

Supporting Evidence:……..

Customer Signature:……

Date:……

Transaction Approved? Yes No

If No, state reason:……
……

…… ……..

OFFICER COMPLETING TRANSACTION AUTHORISING OFFICER

(Signature & Title) (Signature & Title)

Appendix 9

Suspicious/Unusual Transaction Report

SUSPICIOUS / UNUSUAL TRANSACTION REPORT

PLEASE WRITE IN BLOCK LETTERS

IMPORTANT: Complete using information obtained during normal course of the transaction. The report should be completed as soon as practicable AFTER the dealing, and a copy forwarded to:
THE DIRECTOR
ANTI-MONEY LAUNDERING AUTHORITY
P.O. BOX 1372 Bridgetown, Barbados
FACSIMILE NO. (246) 436-4756
Email: amla@sunbeach.net
For urgent reporting – Tel. (246) 436-4734/5

PART A Identity of customers involved in transaction

CUSTOMER 1	CUSTOMER 2 (if more than one customer at counter)
1.:…… (Given names and surname)	**1**.:…… (Given names and surname)
2.:…… …… (Address)	**2**.:…… …… (Address)
3.:…… (Nationality – if not Barbadian)	**3**.:…… (Nationality – if not Barbadian)
4.:…… (Occupation)	**4**.:…… (Occupation)
5.:…… (Date of birth)	**5**.:…… (Date of birth)
6.: Type and number of affected accounts …… ……	**6**.: Type and number of affected accounts …… ……
7.: Particulars of ID, e.g. National ID no., bank account no. ……	**7**.: Particulars of ID, e.g. National ID no., bank account no. ……

PART B Name of account holder

(To be completed only if transaction was conducted on behalf of another person other than those mentioned in part A)

8.:…..……..……..……..…….
(Given names and surname)

9.:……..……..……..…….

……..……..……..…….
(Address)

10.:……..……..……..……..
(Nationality – if not Barbadian)

11.:……..……..……..……..
(Occupation)

12.:……..……..……..……..
(Date of birth)

13.: Type and number of affected accounts

……..……..……..……..

……..……..……..……..

14.: Particulars of ID, e.g. National ID no., bank account no.

……..……..……..……..

……..……..……..……..

PART C Transaction details

15……..……..……..…….
Type of transaction (e.g. deposit, purchase travellers' chq)

16. ……..……..……..…….
(Date of transaction)

17. ……..……..……..……..
(Amount of transaction ($BC)

18. ……..……..……..……..
(If foreign currency involved, name)

19……..……..……..……
(Cheque / transfer /money order / etc)

……..……..……..……
(Name of drawer / Ordering customer)

……..……..……..……
(Name of payee / beneficiary)

20. Other bank involved (if applicable)–name/branch/country

……..……..……..……

……..……..……..……..

PART D Grounds for suspicion (and description if appropriate)

21. Give details of the nature of and circumstances surrounding the transaction and the reason for suspicion

(PLEASE WRITE IN BLOCK LETTERS)

……

……

……

……

……

……

……(If insufficient space, attach a separate statement)

22. If additional information is attached, tick this box ☐

FIU USE ONLY

23. If identity of the customer has not been established in PART A, and they are not known to the officer, give a description (e.g. sex, approximate age, height, build, complexion, etc.)

……

……

……

……

PART E Details of financial institution/place of transaction

24. Type of cash dealer: BANK Cr. Union
Other (describe)
……

25. Organisation……..

26. Branch……

27. Address of Branch ……

……

28. Signatory……

29. Title/Position……

30. Dealers Internal reference number……